Public Knowledge

October 21, 2016

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: WC Docket No. 16-106

Dear Ms. Dortch:

On October 20, 2016, Harold Feld and Dallas Harris of Public Knowledge (collectively "PK") met with Travis Litman of Commissioner Rosenworcel's Office with regard to the above captioned matter.

Browser History and Application History Must Be Classed As Sensitive

If the Commission adopts the sensitive/non-sensitive framework, it is imperative that browser history and application history – what people do online and where they go – must be classed as sensitive. It is not merely that, as PK explained in its Comments[1], because browser history and app history contain both sensitive and non-sensitive information, requiring the carrier to examine the information and therefore exposing the sensitive information to discovery. Rather, ***the entire purpose*** of Section 222[2] – as well as Sections 338(i),[3] 631[4] and 705[5] -- is ***explicitly to protect the confidentiality of communications.*** The browsing history and application history are, in the words of Section 705(a), information pertaining to the "existence, content, purport, effect or meaning" of "any interstate communication by wire and radio."

Section 705 and its capacious protection to the privacy of the actual communication itself, including an information relating to the content such as browser history or application history, predates even the Communications Act of 1934 itself, being a provision of the Federal Radio Act of 1927. The basic principle animating Section 705 is even older, embodying the laws that prohibit mail carriers from recording and using information provided to mail carriers to make mail service possible. Likewise, the capacious privacy protections of the Cable Privacy Act embodied in Section 631 explicitly prohibits any disclosure that would disclose "directly or ***indirectly*** the extent of any viewing ***or other use*** by the subscriber of a cable service ***or other***

[1] See Public Knowledge Comments at 24.
[2] 47 U.S.C. §222.
[3] 47 U.S.C. §338(i)
[4] 47 U.S.C. §551
[5] 47 U.S.C. §605

service provided by the cable operator, or ***the nature of any transaction*** made by the subscriber over the cable system of the cable operator."[6]

"Browser history" and "application history" – for all they use the term history – are the real time recording of communications. They are valuable to the ISP and to 3rd parties precisely because they provide information relevant to the "existence" of the communication, information relevant to its content or effect. The entire purpose of the ISP collecting the information is to both directly and indirectly determine the nature of the subscriber's use of the broadband service and to identify any transactions conducted using this service – often in combination with any cable video service provided.[7]

Section 222 was designed by Congress to compliment and enhance these existing provisions of the Act – not implicitly repeal or curtail them. Any interpretation of Section 222 cannot rationally be read as intending to implicitly repeal longstanding protections that were core parts of both the regulation of communications and the regulation of cable and cable services since the first statutes enacted by Congress explicitly addressing communications by wire and radio in 1927 and cable services in 1984. *See e.g. Am. Trucking Associations, Inc. v. F.C.C.*, 377 F.2d 121 (D.C. Cir. 1966); *Food & Drug Admin. v. Brown & Williamson Tobacco Corp.*, 120 S. Ct. 1291 (2000).

The Commission may certainly, if it chooses, seek to harmonize its overall interpretation of Section 222 with the Federal Trade Commission's interpretation of Section 5 of the Federal Trade Commission Act (FTCA)[8] as those general provisions apply to privacy. But it is the Communications Act, which governs the rules adopted by the Commission, and its interpretation of Section 222 must be consistent not merely with the plain statutory language and legislative history of Section 222, but with its own longstanding interpretation of other Communications Act provisions. *Am. Trucking Associations, Inc.,* 377 F.2d 121.

The Carriers Fundamentally Misconstrue The FTC 2012 Report

Opponents of protecting browser history rely entirely on the FTC's policy guidance statement adopted by the FTC in 2012[9]. The Federal Trade Commission interpretation of 45

---

[6] 47 U.S.C. §§551(c)(2)(ii)(I)-(II) (emphasis added). 47 U.S.C. §551(a)(2)(B) defines "other service" as "any wire or radio communications service using an facilities of a cable operator that are used in provision of cable service." This clearly includes broadband service.

[7] For examples of carrier conduct in violation of the relevant provisions of Section 551, including the intermingling of broadband data and cable viewing data. *See e.g.* In the Matter of Public Knowledge et. al, Petition for the Federal Communications Commission to Enforce Cable Privacy Rules Against Comcast, AT&T, and Cablevision ("Cable Privacy Petition") (June 9, 2016).

[8] 45 U.S.C. §15.

[9] Federal Trade Commission Report, Protecting Consumer Privacy in an Era of Rapid Change (March 2012) ("FTC 2012 Report"), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

U.S.C. §15 to matters under FTC jurisdiction cannot justify an interpretation of 47 U.S.C. §222 which would violate the express provisions of 47 U.S.C. §551 and 47 U.S.C. §605.

Indeed, as the FTC 2012 Report itself recognized, the recommended "best practices" did not even constitute an agency interpretation of Section 5 as applied to privacy, let alone an authoritative interpretation of what would constitute "sensitive" or "non-sensitive" data for all time under all circumstances for all agencies. [FTC 2012 Report at 1. ("The framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.")] In particular, the FTC recognized that its framework was designed to compliment and "work in tandem" with "sector specific regulation" such as 47 U.S.C. §§222, 551 and 605. [Report at 16] While in 2012 BIAS service was not subject to 47 U.S.C. §222, it certainly was subject to 47 U.S.C. §§338(i), 551, 605 and 1302. Despite the efforts of the BIAS industry, advertisers, Google and the technology industry generally to elevate the FTC's 2012 Report from a guide to "encourage best practices" [FTC 2012 Report at 1] to a permanent safe harbor, the 2012 FTC Report by its own words makes clear that it was never designed to supplant the FCC's own interpretation if its own jurisdictional statute. Rather, as the Report made clear, the Framework adopted by the FTC in 2012 represented a generally applicable framework designed to provide a "baseline" for all data – both online and offline – subject to future developments in the market and the law and the interpretation by other agencies of their "sector specific" statutes. [FTC 2012 Report at 16.][10]

Carriers Distort The FTC 2012 Report Recommendations With Regard To BIAS.

It is with this understanding of what the FTC 2012 Report actually sought to achieve that the Commission should interpret the discussion in the Report of BIAS and its relationship to other "platforms" such as search engines and operating systems. [FTC 2012 Report at 55-57] Carriers seek to elevate as holy and immutable writ the determination that the best practices framework adopted should "technology neutral" with regard to BIAS and other platforms capable of tracking both browser history and application history. [FTC 2012 Report at 56] But even if the FTC 2012 Report were a definitive interpretation by the FTC of Section 5 of the FTCA, which by its own terms it is not, and even if such an interpretation could overrule the express provisions of Sections 222, 338(i), 641 and 705, which it cannot, the express language of the discussion of BIAS and other large platform operators makes clear that the FTC recognized that its recommendation on technology neutrality was temporary and limited to its understanding of the market and existing technology in 2012. [Id., *See also* Rousch Dissent at C-7]

The relevant section of the FTC 2012 Report observes that BIAS provider are "in a position to develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible. In addition, it may be difficult for some consumers

[10] *See also* Public Knowledge, *Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World* at 25-42 (explaining complimentary roles of FTC and FCC.), *available at* https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper.pdf.

to obtain alternative sources of broadband Internet access, and they may be inhibited from switching broadband providers for reasons such as inconvenience or expense." [FTC 2012 Report at 56] While adhering to technical neutrality in the short term, the FTC 2012 Report also concluded that other platforms "currently are not so widespread that they could track a consumer's every movement across the Internet." [Id.] So that while the FTC believed that tracking by large platforms such as operating systems and search engines "warrants consumer choice, the [FTC] does ***not*** believe that such tracking currently raises the same level of privacy concerns as those entities that can comprehensively track all or virtually of a consumer's online activity [*i.e.*, ISPs]." [Id., emphasis added.]

It is difficult to understand how ISPs can read this language and celebrate the FTC 2012 Report as sacred and unchanging writ, given their voluminous record filings maintaining that the FTC Report is factually mistaken in its conclusion. Indeed, even the FTC did not make the same claim to infallibility through the ages that its former Chairman now makes as a lobbyist on behalf of the industry.[11] To the contrary, the relevant section of the FTC 2012 Report ultimately concluded that "[t]hese are complex and rapidly evolving areas, and more work should be done to learn about the practices of all large platform providers, their technical capabilities with respect to consumer data, and their current and expected uses of such data." [FTC 2012 Report at 56.] As if to accent just how much has changed since 2012, the FTC 2012 Report explicitly disclaims that ISPs use their tracking ability to "build profiles for marketing purposes" – which would raise grave privacy concerns and require express consent. Id. at n. 269. According to BIAS providers in 2016, however – as well as copious other evidence submitted in the record – building detailed profiles of subscribers for marketing purposes without express consent of the subscribers is exactly what ISPs do today!

In short, the FTC 2012 Report acknowledged quite clearly that this was a rapidly evolving area and that its decision to keep its framework "technology neutral" as between ISPs and other platforms was an administrative preference based on the marketplace as it existed in 2012. Even in 2012, however, the FTC had grave concerns that ISPs were capable of capturing a far more complete and comprehensive picture of the details of people's lives than any search engine or operating system,[12] and warned that if ISPs were capable of constructing detailed profiles of subscriber behavior for marketing purposes it would require opt in protections. The carriers and their advocates have sought to cherry pick from the FTC 2012 Report the one sentence they find convenient, the 2012 decision to make the framework technology neutral, while contesting the factual predicate on which that decision was based.

Contrary To BIAS Provider Assertions, Existing Carrier Practice of Examining Information To Determine Sensitivity, Making An Unreviewed And Unchallengeable Determination As To What Browser or Application History Is "Sensitive," And Acting As It

[11] *See* http://www.broadcastingcable.com/news/washington/ex-government-officials-push-fcc-toward-ftc-privacy-model/160141, http://www.theatlantic.com/politics/archive/2015/05/the-privacy-coalition-that-wants-to-trim-data-regulations-for-telecom-giants/456477/

[12] *See also* Rousch Dissent at C-7 (noting that the FTC was treating ISPs differently from other platforms and justifying the distinction based on broadband provider market power).

Sees Fit Has Never Been Approved By The FTC and Is Subject To Pending Complaints At the FTC and the FCC.

As part of this effort to portray the FTC's 2012 Report as an immutable safe harbor, the carriers assert that their current collection practices have fully complied with FTC rules with no consumer harm or even consumer complaints. This is both factually false and – based on what little the carriers have elected to disclose in the public record as to how carriers sort information into "sensitive" and "non-sensitive" categories – utterly wrong.

As described in the record, carriers appear to practice some form of "white listing" of information that falls into one of the categories the FTC has traditionally designated as "sensitive." While it might seem humorous to ask how an ISP determines whether it classifies whether downloading information on erectile dysfunction cures as "medical" and therefore sensitive, the question of allowing the ISP to make a determination take a grim turn if it tracks visits to websites pertaining to depression. Academic research and therefore safe to sell to any third party? Or medical and therefore requiring opt in? Does the purchase from an online pharmacy of medications – itself surely sensitive – inform the ISPs determination that the web browsing history is likely related to an actual medical condition?

No one knows. Certainly not the subscriber, to whom the ISP currently discloses no more than that it *may* collect some information and that it *may* disclose those to third parties for whatever purposes the ISP sees fit, subject to change in the notice on the ISPs website. Carriers assert that the lack of FTC enforcement actions or consumer complaints demonstrates that their subscribers find this state of affairs entirely satisfactory – and that the FTC has blessed it as complying with Section 5.

As an initial matter, of course, consumers ***have*** complained about ISP data collection practices. Public Knowledge filed precisely such a complaint with both the FTC and the FCC some months ago.[13] A copy of this complaint (previously filed in the record) is attached as a not-so-gentle reminder that the carrier practices are not universally welcome so much as incredible difficult to discover.

Similarly, the claims by carriers that the FTC has approved of these practices is profoundly disingenuous. As the carriers are well aware, the FTC has no rulemaking authority. It has provided no advisory opinion with regard to these carrier sorting practices. Neither has the agency made any other official declaration. The most that carriers can say of their practices under the FTC's Section 5 standard (under which the FTC has the burden of proof, subject to the limiting factors in Section 5(n)) is that the FTC for whatever reason has not processed a complaint.

Or, in other words, BIAS providers seek to convert "we've never been investigated or convicted by the FTC" into a formal declaration of FTC approval. This is simply absurd. To the extent carriers have disclosed their "white listing" processes, they raise grave concerns as to

[13] See Cable Privacy Petition, supra fn 7.

violations of both 47 U.S.C. §551 and 47 U.S.C. §605 – let alone whether they are sufficient safeguards under Section 222.

As the Commission has determined previously in the context of Section 222, a carrier faces an inherent conflict of self-interest when determining whether to use a CPNI for its own purposes or comply with its responsibilities under the Act. *Verizon California, Inc. v. FCC*, 555 F.3d 270 (2008) (inherent conflict with regard to using port request for marketing and expeditiously processing the number port request justifies prohibition on retention marketing until port completed). Here, the inherent conflict of interest for the BIAS provider is plain. The BIAS provider has every incentive to classify information as non-sensitive rather than sensitive. Added to this conflict of interest is the security that the subscriber is utterly unable to in any way audit or investigate the ISP's classification mechanism so as to file a complaint or even protest. The carriers have not even submitted sufficient detail into the record to allow participants in this proceeding to comment on the adequacy of the carriers' sorting mechanisms – or to allow the Commission to make its own evaluation.

Finally, carriers have in the past proven poor judges of what meets the FCC's standards under Section 222. Verizon, for example, engaged in its "Supercookie" program for two years, using a hash to track their mobile customers' browsing history.[14] The Commission rejected the argument that because Verizon had engaged in this conduct for two years and the FTC took no action during that time, that Verizon's conduct was in compliance with Section 222. To the contrary, as part of the settlement, Verizon agreed to refrain from using any similar tracking method without express opt in consent.

To conclude, when BIAS providers insist that consumers and the FTC regard their current practices for separating sensitive browsing history from non-sensitive browsing history, they are drastically overstating the reality. Nor have they provided sufficient evidence to allow the Commission to judge the adequacy of these methods for itself. The inherent self-interest in allowing the ISP to make the decision on what information it can exploit without express consent undermines any confidence consumers or the Commission can have in what amounts to little more than a reassurance to "trust us." Only by classifying browser history and application history as sensitive, and thus requiring opt in to access this information, can the Commission adequately protect the proprietary information of subscribers as required by Section 222.

Prohibiting BIAS Providers From Reviewing Browser And Application History By Designating Browser And Application History As Sensitive Is The Least Restrictive Means of Assuring The Important Government Interests At Stake Here.

The same conflict of interest discussed above also refutes any lingering First Amendment challenge. As even the carriers must concede at this point, given their embrace of the sensitive/non-sensitive framework, the proper standard for analyzing the First Amendment questions is the familiar test found in *Central Hudson Gas and Electric Corp. v. Public Service Commission*, 447 U.S. 557 (1980). To meet this standard the government regulation must advance

[14] Order, *In the Matter of Cellco Partnership, d/b/a Verizon Wireless,* 31 FCC Rcd. 1843 (2016).

a substantial government interest and "the regulation must not be more extensive than is necessary to advance that interest." *NCTA v. FCC*, 555 F.3d 996, 1000 (D.C. Cir. 2009) (internal citations omitted). The government does not need to show that it has adopted the least restrictive means possible, it only must show that the regulation be "proportionate to the interests to be advanced." *Id.*at 1002.

In *Verizon of California supra*, the D.C. Circuit found that resolving the conflict of interest between the carrier's desire to market to a departing customer and expeditiously processing a request to port a phone number to another carrier was sufficient to justify a total ban on marketing to the customer until after the number port request was completed. *Verizon of California*, 555 F.3d at 274-75. Here, the conflict of interest if far more obvious, far more difficult to police, and undermines the far more substantial government interest in preserving consumer privacy. Additionally, as the D.C. Circuit has repeatedly found, "opt out is only marginally less intrusive than opt in." *NCTA,* 555 F.3d at 1002 (citations omitted).

By contrast, any alternative scheme to ensure that carriers were properly classifying information as sensitive or non-sensitive would be far more intrusive and unlikely to work as well. That two mobile carriers, Verizon and AT&T, were able to track ***all*** web history, sensitive and non-sensitive, for two years without discovery indicates the enormous difficulty in policing this conduct. The Commission would need to require pre-certification, or conduct spot inspections, or otherwise engage in constant vigilance with accompanying production burden on the ISPs to determine if the ISP were properly distinguishing between sensitive and non-sensitive information.

Designating Browser History And Application History As Non-Sensitive Would Undermine The Recent Data Privacy Shield Agreement Between The US and the EU, Jeopardizing The Ability of US Residents and Businesses To Send or Receive Information From EU Residents.

In 2015, in the wake of the Snowden revelations, the EU Court of Justice struck down the existing agreement between the United States and the EU that permitted companies to transfer personal information out of Europe to the United States consistent with the EU Privacy Directive.[15] The United States Department of Commerce and the European Union negotiated a new "Privacy Shield" agreement that relies upon regulations, self-certification and enforcement in the United States to provide adequate standards of protection for personally identifying information (PII) of European citizens.[16] Whether the EU Court of Justice will consider the Privacy Shield adequate remains to be seen.

An additional complication has emerged within the last week as the EU Court of Justice has determined that dynamic and static IP addresses are PII subject to the EU Privacy Directive

[15] https://www.wired.com/2015/10/tech-companies-can-blame-snowden-data-privacy-decision/

[16] https://www.commerce.gov/page/eu-us-privacy-shield, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf.

and therefore, of course, subject to the restrictions of Privacy Shield. The proposed treatment of browser history and application history as "non-sensitive," appears likely to significantly undermine the adequacy of the Privacy Shield for the EU Court of Justice. By contrast, treatment of browser history and application history as sensitive information will likely enhance the acceptability of the Privacy Shield.

To understand why, it is important to keep in mind two things. First, "browser history" and "application history" are a stored collection of IP addresses and associated metadata. They are valuable precisely because the IP address identifies the source or destination of the transmission.[17] Second, by tracking browser history and application history without express consent, by storing and examining application history and browser history for traffic inbound from the EU or outbound to the EU, ISPs store and use EU PII without regard to the Privacy Shield. Worse for US companies that do certify under Privacy Shield, their information must invariable pass through ISPs (third parties) who have access to the IP addresses inbound from or outbound to the EU.

PK does not state definitively that classifying IP addresses – whether as part of browser history or application history – automatically violates the requirements of the Privacy Shield. Rather, PK urges that the Commission implement the regulatory regime that is most conducive to compliance with the EU Privacy Directive and Privacy Shield. Under Section 303(r), the Commission has both the authority and the responsibility to implement the provisions of any international agreement relating to communication by wire and wireless.[18] At a minimum, the Commission should avoid adopting a regulatory framework for ISP privacy which would raise a cloud over the Privacy Shield when it has only just been agreed to and implemented.

Designating Brower and Application History As Non-Sensitive Will Undermine Longstanding Protections For Call History, Cable Viewing History, and Other Traditionally Protected Information When The Commission Harmonizes These Regulations With The Broadband Privacy Regulations.

Finally, the Commission must consider the implications of classifying browser history and application history as non-sensitive unless they clearly relate directly to a category of sensitive information. Carriers have enthusiastically urged the Commission to harmonize existing CPNI and cable privacy regulations with the framework adopted in this proceeding (assuming that the Commission adopts the framework the carriers favor). Once the Commission establishes that the record of web sites visited and services used is not sensitive, it inevitably follows that call record history, video channel viewing, and other information traditionally protected under Section 222

[17] PK does not assert that an IP address or other identifier is proof positive of identification in all circumstances. Indeed, the ability to forge an IP address is well established. But the ISP is in a unique position to use the IP address as an identifier because it is the ISP that assigns the IP address (in the case of a dynamic IP address) and that completes the routing to the end user.

[18] 47 U.S.C. §303(r). Accordingly, even though the Commerce Department is charged under the agreement with ensuring compliance with the certification regime, the FCC has both a statutory authority and responsibility to ensure that the United States properly implements Privacy Shield with regard to the actual transfer of data.

and Section 631 would become accessible to cable operators, telephone providers, VOIP providers, and to third parties with whom they wish to share this information.

This cuts two ways. First, if the Commission intends to maintain the existing protection for call records – whom Americans call, how often, and other metadata that has traditionally received the highest level of protection – it must have some rational basis for distinguishing call history from browsing history, or cable viewing from video streaming. Second, if the Commission classifies browser and application history as non-sensitive, it should make clear that consumers will be stripped of the privacy protections which they trust and value.

The Commission Has Both The Authority And The Evidence In The Record To Prohibit Mandatory Arbitration Clauses For Violations of Its Privacy Regulations.

In the wake of the Ninth Circuit's recent decision in *AT&T Mobility v. FTC*, the Commission has lost a valuable partner in protecting the privacy of broadband subscribers. Furthermore, the Commission relies exclusively on private rights of action and class actions to enforce MVPD privacy under 47 U.S.C. §§ 338(i) & 551. Without the ability to sue for relief in court, consumers have no replacement for the loss of the FTC as a partner with the FCC. Furthermore, the proliferation of mandatory arbitration clauses effectively forecloses consumers from enforcing their rights under 47 U.S.C. §§ 338(i) & 551.

There is evidence in the record documenting the ubiquity of mandatory arbitration clauses in telecommunications service contracts and the harm they cause to consumers.[19] In addition to the evidence in the record, the Consumer Financial Protection Bureau conducted a three- year examination on the use of forced arbitration in the consumer financial services sector.[20] The study data and agency findings are a strong indicator of how forced arbitration impacts customers in telecommunications, including for broadband privacy claims.

Prohibiting mandatory arbitration clauses is particularly warranted in this context for several reasons. Section 222 and 47 U.S.C. §§ 338(i) & 551 are inextricably linked. The cable privacy provisions apply to any service that is delivered over the same infrastructure, which includes broadband. The Commission has long relied on private rights of action to enforce the 47 U.S.C. §§ 338(i) & 551. Because of the connection between the privacy provisions, allowing mandatory arbitration clauses in privacy policies would have an impact on consumer's privacy rights beyond 47 U.S.C. § 222. Further, ISPs maintain consumer information and assume the risk by demanding that consumers opt-out instead of opt-in. If ISPs insist on collecting large amounts

[19] *See e.g.*, NACA et al. Notice of Ex Parte, WC Docket No. 16-106 (filed September 22, 2016); Comments of National Association of Consumer Advocates, et al.; New America's Open Technology Institute, ACLU, Free Press, Center for Democracy & Technology, Center for Digital Democracy, Common Sense, Electronic Privacy Information Center, Consumer Federation of America, Consumer Watchdog Notice of Ex Parte (filed September 12, 2016).

[20] Consumer Financial Protection Bureau, Arbitration Study: Report to Congress 2015, *available at* http://www.consumerfinance.gov/data-research/research-reports/arbitration-study-report-to-congress-2015/ .

of consumer data on an opt-out basis, they must be accountable to consumers when their privacy is violated.

The Commission should therefore use its authority pursuant to Section 201(b), 338(i) and 631 to prohibit enforcement of mandatory arbitration clauses. At a minimum, even if the Commission were to determine that it did not intend to prohibit such clauses based on the record, the Commission should clarify that it has such authority and will revisit its determination if evidence of the abusive effects of these clauses becomes more manifest.

In accordance with Section 1.1206(b) of the Commission's rules, this letter is being filed with your office. If you have any further questions, please contact me at (202) 861-0020.

Respectfully submitted,

/s/ Harold Feld
Harold Feld
Senior V.P.
Public Knowledge
1818 N Street, NW
Washington, DC 20036

Cc: Matthew Delnero
Lisa Hone
Ruth Milkman
Gigi Sohn
Jennifer Tatel
Claude Aiken
Travis Litman